CORE
Metadata, citation and similar papers at core.ac.uk
Provided by University of Kentucky

Kentucky Law Journal

Volume 94 | Issue 2 Article 6

2005

Neither Big Brother Nor Dead Brother: The Need for a New Fourth Amendment Standard Applying to Emerging Technologies

Casey Holland
University of Kentucky

Follow this and additional works at: https://uknowledge.uky.edu/klj

Part of the Communications Law Commons, Fourth Amendment Commons, Law Enforcement and Corrections Commons, and the Privacy Law Commons

Right click to open a feedback form in a new tab to let us know how this document benefits you.

Recommended Citation
Holland, Casey (2005) "Neither Big Brother Nor Dead Brother: The Need for a New Fourth Amendment Standard Applying to Emerging Technologies," *Kentucky Law Journal*: Vol. 94 : Iss. 2 , Article 6.
Available at: https://uknowledge.uky.edu/klj/vol94/iss2/6

This Note is brought to you for free and open access by the Law Journals at UKnowledge. It has been accepted for inclusion in Kentucky Law Journal by an authorized editor of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.

Neither Big Brother Nor Dead Brother: The Need for a New Fourth Amendment Standard Applying to Emerging Technologies

Casey Holland[1]

On each landing, opposite the lift shaft, the poster with the enormous face gazed from the wall. It was one of those pictures which are so contrived that the eyes follow you about when you move. BIG BROTHER IS WATCHING YOU, *the caption beneath it ran* ....

....

... The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. ... How often, or on what system, the Thought Police plugged in on any individual wire was guesswork.[2]

—George Orwell, 1984

We're talking about the balance between privacy, on the one hand, and protection from Big Brother government, but we're also talking about the government's responsibility to protect our people. It comes down to the choices, my staff has said to me many times, between Big Brother and dead brother. And I think our first responsibility in government is to make sure we don't have any more dead brothers.[3]

—Porter Goss, Director
Central Intelligence Agency

BIG BROTHER casts an ominous shadow over any new type of surveillance technology.[4] Often, privacy advocates view technical advancements in

1 J.D. expected 2006, University of Kentucky; B.A., Political Science, University of Kentucky, 2003. I would like to extend my heartfelt gratitude to the following: Dr. Bradley Canon, for supporting my first forays into Fourth Amendment issues; Prof. William Fortune, for his helpful comments and encouragement on an early draft; my colleagues on the editorial board of the *Kentucky Law Journal*, for their tireless assistance in making this a better piece; and my father, Archie Holland, for answering an unending stream of questions about network architecture.

2 GEORGE ORWELL, 1984, at 5–6 (Signet Classic 2000) (1949).

3 *All Things Considered: Profile: Porter Goss is Nominated to be Director of the Central Intelligence Agency* (National Public Radio broadcast Aug. 10, 2004).

4 Both the Supreme Court and commentators have proven remarkably prescient on this

monitoring as Orwellian evils.[5] Concurrently, law enforcement and anti-terrorism advocates routinely see the lack of expanded technological means of covert observation as an invitation to utter disaster.[6] This Note posits that there is an alternative to the Big Brother–dead brother diametric view; that emerging technologies can be used to protect national security without endangering longstanding constitutional values.

Due to the nature of scientific development, the controversy over emerging surveillance technologies is a relatively recent one. For decades, the paradigm of law enforcement's use of investigatory devices was the classic wiretap.[7] Since then, electronic innovations have launched a revolution in the use of digital devices to observe and record the activities of others. Pen register/trap and trace devices,[8] digital pager clones,[9] keylogging

---

point. *See* Olmstead v. United States, 277 U.S. 438, 474 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967) (Brandeis, J., dissenting) ("The progress of science in furnishing the government with means of espionage is not likely to stop with wire–tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."); *see also* CONFERENCE ON THE BOUNDARIES OF PRIVACY IN AMERICAN SOCIETY, FINAL REPORT 2 (1972) (Samuel Alito, chairman), http://www.epic.org/privacy/justices/alito/report110205.pdf ("The cybernetic revolution has greatly magnified the threat to privacy today....The potentional for invasion of privacy through the use of computers is growing rapidly....Centralization, the creation of vast computer networks, opens the possibility of bringing together an enormous amount of information about every facet of an individual's life."); Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's*, 66 COLUM. L. REV. 1003, 1006–08 (1966), *excerpted in* RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS 82–83 (1999) (describing numerous developments in surveillance technology); Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890), *excerpted in* TURKINGTON & ALLEN, *supra*, at 30 ("Recent inventions ... call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone.'"). The Warren and Brandeis article later provided the foundation for the recognition of tortious invasion of privacy claims. *See* RESTATEMENT (SECOND) OF TORTS § 652A cmt. a (1977).

5 *See, e.g., Security and Liberty: Protecting Privacy, Preventing Terrorism: Hearing Before the Nat'l Comm'n on Terrorist Attacks Upon the United States*, 108th Congress 1 (2003) (statement of Marc Rotenberg, President, Electronic Privacy Information Center), http://www.epic.org/privacy/terrorism/911commtest.pdf (referring to "Big Brother databases").

6 *See, e.g., supra* note 4 and accompanying text.

7 *See Olmstead*, 277 U.S. at 456–57; Katz v. United States, 389 U.S. 347, 348 (1967) (Congress codified the *Katz* principles in the Electronic Comminucations Privacy Act, 18 U.S.C. § 2510 (1968)).

8 *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 161 (1977); Smith v. Maryland, 442 U.S. 735, 737 (1979), *superseded by statute*, Pen Registers and Trap and Trace Devices, Pub. L. No. 99-508, Title III, § 301(a), 100 Stat. 1871 (Oct. 21, 1986). A pen register is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted," while a trap and trace is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information." 18 U.S.C. § 3127(a) (2000).

9 *See* Brown v. Waddell, 50 F.3d 285, 287 (4th Cir. 1995). A digital pager clone is a device

programs,[10] packet-sniffing systems,[11] and biometric identifiers[12] have all become fairly common tools of law enforcement agencies. The reason that so many digital surveillance techniques have developed in recent years is simple: as a tool for both common criminals and international terrorists, the Internet has exploded as the primary means of communications.[13] Child pornographers, mobsters, con men, and even terrorists have turned to the Internet for anonymity and safety from investigatory agencies.[14] It is a truism that some form of electronic communications surveillance is necessary not just to investigate criminal behavior but to prevent future terrorist attacks. The Supreme Court itself recognized this decades ago:

> The marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission, and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its law-abiding citizens.[15]

Of course, a rift emerges with respect to the specific surveillance utilized and its method of utilization. As a philosophical matter, the Orwell-Goss division generally falls into a classical libertarianism-communitarianism structure, the former valuing individualism and personal autonomy, the latter primarily concerned with social responsibility and the common good.[16]

---

to "monitor numeric messages received" on another's pager. *Id.* at 286.

10 *See* United States v. Scarfo, 180 F. Supp. 2d 572, 574–75 (D.N.J. 2001). Keyloggers include such systems as the FBI's "Magic Lantern," a "virus-like program" that records keystrokes and can hence be used to discover encryption passwords. *See* James Adams, *Suppressing Evidence Gained by Government Surveillance of Computers*, 19 CRIM. JUST. 46, 48–49 (2004).

11 *See generally* Casey Holland, *The Carnivore Internet Monitoring Device: Capabilities, Statutory Framework, and Constitutional Considerations, excerpted in* 2 KALEIDOSCOPE: U. KY. J. UNDERGRADUATE SCHOLARSHIP 34 (2003), *available at* http://www.uky.edu/Kaleidoscope/fall2003/oswald/holland-article.pdf. Packet sniffers are either hardware or software that record digital information transmitted over a computer network. For definitional purposes only, packet sniffers as Internet surveillance devices are roughly analogous to traditional wiretaps on telephone lines. *See id.* at 4–5.

12 *See* AMITAI ETZIONI, THE LIMITS OF PRIVACY 115–20 (1999). A biometric identifier "analyzes and measures unique physiological or biological characteristics" for identification purposes. *Id.* at 115 (internal citation omitted).

13 *See The "Carnivore" Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the Subcomm. on the Const. of the H. Comm. on the Judiciary*, 106th Cong. 9 (2000), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_senate_hearings&docid=f:74729.pdf (statement of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation) [hereinafter *Hearings*].

14 *See id.* at 9–10.

15 United States v. U.S. Dist. Court, 407 U.S. 297, 312 (1972).

16 *See generally* ETZIONI, *supra* note 12; *see also* Gaia Bernstein, *Accommodating Technological Innovation: Identity, Genetic Testing, and the Internet*, 57 VAND. L. REV. 965, 975–79 (2004) (describ-

As a constitutional matter, the same schism is primarily addressed in one context: the Fourth Amendment.[17] Unfortunately, as is so often the case with questions of constitutional interpretation, the Fourth Amendment offers no easy answers to the question of whether new surveillance technologies can be used by law enforcement without a warrant.[18] Part I of this Note will examine the various ways in which new law enforcement tools and techniques have been analyzed under the Fourth Amendment and address the benefits and detriments of evaluating emerging technologies under each constitutional standard.[19] Part II will apply the various standards to a test case, the monitoring of electronic mail ("e-mail").[20] Finally, Part III will propose a new, merged standard that will satisfy the concerns of both privacy advocates and law enforcement officials.[21] This merged standard will provide strong protections for individual privacy while offering the flexibility necessary to adequately protect national security. By putting forward such a proposal, this Note offers an alternative that is neither Big Brother nor dead brother but is a median approach repudiating both.

I. CURRENT FOURTH AMENDMENT STANDARDS APPLYING TO EMERGING TECHNOLOGIES

Generally speaking, there is only one Fourth Amendment search and seizure requirement and that is reasonableness.[22] However, under the general

---

ing the competing liberal and communitarian "meta-narratives"). Of course, this is an essentialized version of the philosophical debate over privacy and countless other viewpoints exist. *See, e.g.*, Richard A. Posner, *An Economic Theory of Privacy*, REGULATION, May/June 1978), at 19–26 (describing a right of privacy centered around economic concerns). It should be noted that this Note adopts a somewhat Rawlsian approach, implicitly positing that the best way to ensure both privacy and security is to balance the libertarian and communitarian approaches without presuming one's societal position. *See* JOHN RAWLS, A THEORY OF JUSTICE 11–13 (1971), *excerpted in* ROBERT L. HAYMAN, JR. ET AL., JURISPRUDENCE CLASSICAL AND CONTEMPORARY: FROM NATURAL LAW TO POSTMODERNISM 18–19 (Jean Stefancic ed., 2d ed. 2002).

17 *See supra* notes 7–12 and accompanying text.

18 U.S. CONST. amend. IV reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

19 *See infra* notes 22–78 and accompanying text.

20 *See infra* notes 79–131 and accompanying text.

21 *See infra* notes 132–41 and accompanying text.

22 "The things here forbidden are two—search and seizure. And not all searches nor all seizures are forbidden, but only those that are unreasonable." Boyd v. United States, 116 U.S. 616, 641 (1886). Searches conducted without a warrant are, subject to exception, "*per se* unreasonable." Coolidge v. New Hampshire, 403 U.S. 443, 454–55 (1971).

reasonableness rubric, the Supreme Court has used various interpretational techniques and espoused myriad different tests.[23] Among these varying tests, the Supreme Court has utilized three different standards to analyze new surveillance technologies under the Fourth Amendment. The first standard, originally elucidated in Justice Harlan's concurrence in *Katz v. United States*, states that the Fourth Amendment requires a warrant whenever "a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[24] The second standard, from *Kyllo v. United States*, holds that when the surveillance technology used is "not in general public use ... the surveillance is a 'search' and is presumptively unreasonable without a warrant."[25] The third and final standard, expounded in numerous drug-testing and roadblock cases, balances "the nature of the intrusion on the individual's privacy against the promotion of legitimate governmental interests ... beyond the normal need for law enforcement."[26] Each standard has its advantages and disadvantages in the balancing act between privacy and security, and this Note will address these in turn.

A. The Katz *Reasonable-Expectation-of-Privacy Test*

Despite its original presence in Justice Harlan's concurrence in *Katz* as opposed to appearing in the majority opinion, the "reasonable expectation of privacy test" is the primary standard under which the Supreme Court analyzes new law enforcement investigative techniques under the Fourth Amendment.[27] *Katz* and its progeny have the benefit of years of precedential weight behind them under which a number of thorny constitutional issues have already been litigated. Additionally, the *Katz* test is somehow intrinsically pleasing to the sense of balance between privacy and security. The test's very subjectivity, which depends not just on individual subjective manifestations but the subjective manifestations of society in general (as measured by the Supreme Court), essentially provides a constitutional cover for the Court's application of nebulous principles of justice.

23 *See* Kathryn R. Urbonya, *Rhetorically Reasonable Police Practices: Viewing the Supreme Court's Multiple Discourse Paths*, 40 AM. CRIM. L. REV. 1387 (2003).

24 *Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring).

25 Kyllo v. United States, 533 U.S. 27, 40 (2001).

26 Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie County v. Earls, 536 U.S. 822, 829 (2002) (internal quotations omitted).

27 *See, e.g.*, California v. Greenwood, 486 U.S. 35, 39 (1988) ("The warrantless search and seizure of the garbage bags left at the curb outside the Greenwood house would violate the Fourth Amendment only if respondents manifested a subjective expectation of privacy in their garbage that society accepts as objectively reasonable.").

Despite the fact that legal realism takes that premise as a central tenet of its jurisprudential philosophy,[28] the ad hoc nature of the *Katz* test is a serious cause of concern for commentators and even for the Supreme Court itself: "[t]he *Katz* test... has often been criticized as circular, and hence subjective and unpredictable."[29] The *Katz* test is frequently invoked to find that a reasonable expectation of privacy does *not* exist, lending credence to the argument that its progeny are merely extemporized decisions and that the test does little to protect privacy.[30] The Supreme Court has ruled under *Katz* that a person has no reasonable expectation of privacy in conversations conducted before a third party,[31] his or her banking records,[32] the numbers dialed on his or her telephone,[33] the location of his or her automobile,[34] objects and actions observable from aerial surveillance,[35] or the contents of his or her garbage placed on the street for pickup.[36] Still, a more pressing concern than the arguably limited privacy protections provided by *Katz* is its near-total lack of guidance on whether the Fourth Amendment applies to new technologies and investigative techniques. Due to its somewhat unpredictable application, neither private citizens nor law enforcement officers can be reasonably certain whether or not the Fourth Amendment would require a warrant to issue prior to the use of a new technological device. Conceivably, this uncertainty provides for greater privacy protection as law enforcement may be hesitant to utilize a new technology absent a warrant for fear of having critical evidence declared inadmissible.[37] Still, the lack of predictability in the *Katz* standard is potentially injurious to national security. If law enforcement is to have the tools necessary to

28 *See* Jerome Frank, *Are Judges Human?*, 80 U. PA. L. REV. 17, 49 (1931), *excerpted in* HAYMAN ET AL., *supra* note 16, at 195 ("But as the knowledge of rules is a very limited value in the game of guessing future decisions, most legal rights and duties are extremely uncertain, however certain and exact the legal rules.").

29 *Kyllo*, 533 U.S. at 34 (citing 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.1(d) (3d ed. 1996)).

30 *See* Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663, 675–76 (2004).

31 *See* United States v. White, 401 U.S. 745, 749 (1971); *see also* Hoffa v. United States, 385 U.S. 293, 302 (1966) (decided prior to *Katz*).

32 *See* United States v. Miller, 425 U.S. 435, 440 (1976), *superseded by statute*, Right to Financial Privacy Act, Pub. L. No. 95–630, 92 Stat. 3641 (1978) (modified as amended at 12 U.S.C. §§ 3401–3422 (2000)).

33 *See* Smith v. Maryland, 442 U.S. 735, 742–44 (1979).

34 *See* United States v. Karo, 468 U.S. 705, 713 (1984).

35 *See* California v. Ciraolo, 476 U.S. 207, 212–14 (1986).

36 *See* California v. Greenwood, 486 U.S. 35, 39–40 (1988).

37 *See* Weeks v. United States, 232 U.S. 383, 398–99 (1914), *overruled by* Mapp v. Ohio, 367 U.S. 643 (1961) (holding that evidence obtained unconstitutionally must be excluded in both state and federal courts).

combat terrorism, it would be useful to know whether or not a warrant is required either by the Fourth Amendment or by statute.[38]

B. The Kyllo *General-Public-Use Test*

The second reasonableness standard seems specifically adapted to analysis of emerging technologies under the Fourth Amendment. The *Kyllo* case involved the use of a thermal imaging device to observe large heat lamps used in a private residence to grow marijuana indoors.[39] In a ruling that seems tailored to application to new and emerging technology, the Court held that searches with devices not in "general public use" are "presumptively unreasonable absent a warrant."[40] The advantages of such a standard are fairly obvious. As opposed to the *Katz* standard which is subjective and difficult to predict in its application[41] the *Kyllo* test provides a line which is "not only firm but also bright."[42] Privacy protection is obviously paramount in the *Kyllo* decision, yet the clarity of the rule avoids the perils of law enforcement confusion that plague the *Katz* standard which is even less protective of individual privacy. At first glance, then, the *Kyllo* standard appears perfectly suited as a Fourth Amendment rule for new technologies.

Of course, the impression provided by a "first glance" in the constitutional context is misleading and impracticable. As an initial matter, the narrowness of the holding frequently makes *Kyllo* inapposite.[43] Therefore, the decision's legitimacy as a strong constitutional doctrine is questionable.[44]

38 In a number of cases, the Court's decisions that particular searches do not require constitutional procedures have sparked Congressional responses requiring some form of judicial authorization for the search. *See, e.g.*, Right to Financial Privacy Act, Pub. L. No. 95–630, 92 Stat. 3641 (1978) (codified as amended at 12 U.S.C. §§ 3401–3422 (2000)). For further examples, see *infra* notes 83, 91, 95, and 97 and accompanying text.

39 Kyllo v. United States, 533 U.S. 27, 29–30 (2001). It is interesting to note that from a scientific standpoint, no literal intrusion occurred in *Kyllo*. Thermal imagers, like millimeter-wave imagers, parabolic microphones, and van Eck radiation detectors, are entirely passive in nature, detecting only emanations which are "voluntarily provided." Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 535–38 (2005).

40 *Kyllo*, 533 U.S. at 40.

41 *See supra* notes 27–38 and accompanying text.

42 *Kyllo*, 533 U.S. at 40.

43 *See, e.g.*, United States v. Lopez, 380 F.3d 538, 544 (1st Cir. 2004), *cert. denied*, 125 S. Ct. 924 (2005), *and reh'g denied*, 125 S. Ct. 1379 (2005) (declining to extend *Kyllo* to cars); United States v. Hatfield, 333 F.3d 1189, 1195 (10th Cir. 2003) (distinguishing *Kyllo* from the visual search of a fenced-in back yard); United States v. Davis, 326 F.3d 361, 364–66, 366 n.2 (2d Cir. 2003), *cert. denied*, 540 U.S. 908 (*Kyllo* inapplicable to a confidential informant's use of a covert video camera).

44 The Court recently cited *Kyllo* for merely the second time in any context, for the express purpose of distinguishing it. *See* Illinois v. Caballes, 543 U. S. 405, 409 (2005). In Groh v. Ramirez, 540 U.S. 551, 559 (2004), the Court quoted from but did not rely upon *Kyllo*.

Still, even if *Kyllo* is accepted as constitutional writ, it contains a critical limitation: the standard applies only to searches conducted within a home.

> While it may be difficult to refine *Katz* when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portions of residences are at issue, in the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*.[45]

It is on this basis—that *Kyllo* applies only to searches of the portions of a home not visible or otherwise detectable from outside it—that courts have refused to extend the doctrine.[46] Courts' refusal to apply *Kyllo* to general circumstances makes it inapposite as a reliable and widely used test.[47]

There is an added dimension of difficulty in that the constitutional doctrine of *Kyllo* changes with the commonality of use of a particular technology and not with the text of the Constitution or even with shifts in fundamental societal values. This presents a hurdle, albeit not an insurmountable one, for judges favoring originalism as the primary method of constitutional interpretation.[48] There are at least two other constitutional doctrines that either explicitly or implicitly depend on the nature of the technology in present use. The most famous example comes from the Court's abortion decisions in which fetal viability was determined to be the point at which the state interest in protecting fetal life outweighs the individual right to privacy.[49] "To be sure,... there may be some medical developments that affect the precise point of viability, but this is an imprecision within tolerable limits given that the medical community and all those who must

45 *Kyllo*, 533 U.S. at 34.

46 *See, e.g.*, United States v. Allen, 289 F. Supp. 2d 230, 243 (N.D.N.Y. 2003) (declining to apply *Kyllo* to a device used to ascertain discrepancies between power flowing to a house and the power use listed by the electrical meter outside the house); *see also Caballes*, 125 S. Ct. at 838.

47 The distinction between privacy within and without a home is by no means an arbitrary one, as legal history dating to antiquity supports the proposition that "a man's house is his castle." *See* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 13–15 (Da Capo Press 1970) (1937), *excerpted in* TURKINGTON & ALLEN, *supra* note 4, at 7–8 (noting Biblical origins of special privacy protections for the home); *see also* Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.) (striking down a general search warrant of a home), *cited with approval in* Boyd v. United States, 116 U.S. 616, 630 (1886).

48 *See, e.g.*, Antonin Scalia, *Originalism: The Lesser Evil*, 57 U. CIN. L. REV. 849, 855 (1989). That Justice Scalia wrote the majority opinion in *Kyllo* presents an inescapable irony.

49 *See* Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833, 869–70 (1992) (plurality opinion of O'Connor, J.).

apply its discoveries will continue to explore the matter."[50] Another line of cases in which technological development has altered constitutional law involves the validity of prohibitions on "indecent" expression under the First Amendment, as newer technology has increased the ability of individuals to refrain from coming into contact with indecent communications as well as the ability of parents to shield children from them.[51] Thus, while it is concededly disconcerting for a constitutional doctrine to be applied differently depending on the state of technology at the time a case is decided, it is by no means a jurisprudential first.

C. The Legitimate Governmental Interests Test

The third and final standard which the Supreme Court could apply to analyze the reasonableness of new technologies under the Fourth Amendment is the "legitimate governmental interests" test, also called the "special needs" test. Simply stated, the test provides an exception to the ordinary Fourth Amendment warrant requirement for searches when they are conducted, not for law enforcement purposes, but for some other special governmental reason.[52] Such searches need not be supported by a warrant or other judicial authorization, probable cause, exigent circumstances, or even reasonable suspicion, but can in fact be completely suspicionless.[53] Three separate lines of cases support this standard: one relating to random drug testing, another to checkpoints and roadblocks on public highways, and the final one to searches of closely regulated spaces. In the first line of cases, the Court has upheld random drug testing of train conductors,[54] Customs Service agents,[55] student participants in extracurricular sports,[56] and student participants in all extracurricular activities,[57] all in the interest of combating illegal drug use and thereby increasing general public safety. In the second line of cases, the Court has upheld or endorsed roadblocks or checkpoints

50 *Id.* at 870 (internal citations omitted).

51 *Compare* FCC v. Pacifica Found., 438 U.S. 726, 749–50 (1978) (holding that sanction of a radio station for broadcasting indecency is constitutionally permissible), *with* Reno v. ACLU, 521 U.S. 844, 876–79 (1997) (holding that a law illegalizing the dissemination of indecency via the Internet is unconstitutional).

52 "Only in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable, is a court entitled to substitute its balancing of interests for that of the Framers." New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).

53 *See* City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000).

54 *See* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 634 (1989).

55 *See* Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 666 (1989).

56 *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 664–65 (1995).

57 *See* Bd. of Educ. of Indep. Sch. Dist. No. 92 of Pottawatomie County v. Earls, 536 U.S. 822, 838 (2002).

conducting similarly random searches for illegal aliens,[58] drunk drivers,[59] and unlicensed drivers,[60] also in the interest of public safety. However, the Court drew the line at allowing a checkpoint for which the sole purpose was to allow vehicles to be sniffed by a narcotics-detecting dog, since no special need beyond the "general interest in crime control" was ascertainable.[61] In the third and final line of precedent following this balancing approach, the Court has allowed warrantless searches on a general suspicion of probationers' homes,[62] highly regulated businesses,[63] employee desks and offices,[64] students' property at school,[65] and prison inmates' body cavities.[66]

Strictly speaking, the precedents as they currently stand have little if anything to do with the effect of new technology on the Fourth Amendment. However, considering the noticeable effect that terrorism has had on the national consciousness since the attacks of September 11, 2001, it is certainly conceivable that a new "special need" in the form of national security could be proffered as a means to avoid analysis under *Katz* or *Kyllo*. In fact, in the Supreme Court's most recent case finding a warrantless search to be reasonable under the Fourth Amendment, the two *dissenting* Justices indicated that they would have accepted the same search had it been justified by security concerns.[67] Since the unpredictability of the evaluation of new technology under the Fourth Amendment is the impetus to this Note, and since unpredictability in thwarting future terrorist attacks is certainly not a desirable attribute, this probable eventuality merits examination. If national security were adopted as an acceptable alternative to law enforcement interests, the legitimate governmental interest test would mean that the use of surveillance technologies requiring a warrant under normal circumstances could be done without any judicial supervision, so long as it were done in the interest of national security.[68]

58 *See* United States v. Martinez-Fuerte, 428 U.S. 543, 566–67 (1976).

59 *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 455 (1990).

60 *See* Delaware v. Prouse, 440 U.S. 648, 663 (1979).

61 *See* City of Indianapolis v. Edmond, 531 U.S. 32, 41–42 (2000).

62 *See* Griffin v. Wisconsin, 483 U.S. 868, 873–76 (1987).

63 *See* New York v. Burger, 482 U.S. 691, 699–703 (1987).

64 *See* O'Connor v. Ortega, 480 U.S. 709, 721–26 (1987) (plurality opinion).

65 *See* New Jersey v. T.L.O., 469 U.S. 325, 337–42 (1985).

66 *See* Bell v. Wolfish, 441 U.S. 520, 560 (1979).

67 *See* Illinois v. Caballes, 125 S. Ct. 834, 843 n.7 (2005) (Souter, J., dissenting) ("Unreasonable sniff searches for marijuana are not necessarily unreasonable sniff searches for destructive or deadly material if suicide bombs are a societal risk."); *id.* at 847 (Ginsburg, J., dissenting) ("The use of bomb-detection dogs to check vehicles for explosives without doubt has a closer kinship to the [constitutional] sobriety checkpoints in *Sitz* than to the [unconstitutional] drug checkpoints in *Edmond*.").

68 *See* City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) ("[T]he Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack....").

Needless to say, the assertion that the Constitution applies differently in cases of national emergency presents a disquieting proposition for constitutional law. From a historical perspective, however, this has sometimes been the case.[69] Yet, from the same historical perspective, the Supreme Court has often taken a dim view of such actions later affirming the validity of constitutional rights during wartime.[70] Legal scholars are divided on the question of whether the Constitution should apply equally during times of war or national emergency especially where its application could slow law enforcement efforts or even forestall preventing the emergency from occurring.[71] Still, in general terms, Chief Justice Rehnquist has stated that "[i]t is neither desirable nor is it remotely likely that civil liberty will occupy as favored a position in wartime as it does in peacetime."[72] There is, however, no direct legal precedent that war, national security, or terrorism have any effect on the interpretation of the Fourth Amendment in particular. The one Supreme Court case to squarely address the issue roundly denounced the proposition that the government could get around the Fourth Amendment in the name of protecting national security, stating that "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."[73] Other recent cases seem to indicate a similar philosophy.[74] Contrarily, the Foreign Intelligence Surveillance Court of Review

69 Common examples include Lincoln's suspension of habeas corpus rights during the Civil War, the Palmer raids during World War I, the Japanese internment camps during World War II, and McCarthyism during the Cold War. *See* Erwin Chemerinsky, *Losing Liberties: Applying a Foreign Intelligence Model to Domestic Law Enforcement*, 51 UCLA L. REV. 1619, 1619–21 (2004).

70 *See, e.g.*, *Ex parte* Milligan, 71 U.S. (4 Wall.) 2, 120–24 (1866) (striking down Lincoln's suspension of habeas corpus); *see also* New York Times Co. v. United States, 403 U.S. 713 (1971) (per curiam) (holding that the suppression of classified documents concerning the Vietnam conflict from publication was an unconstitutional prior restraint). *But see* Korematsu v. United States, 323 U.S. 214, 219–20 (1944) (upholding the use of Japanese interment camps).

71 *Compare* Ronald M. Gould & Simon Stern, *Catastrophic Threats and the Fourth Amendment*, 77 S. CAL. L. REV. 777 (2004) (specifically endorsing the use of the special-needs test in the context of a search for a nuclear weapon deployed somewhere in the United States), *with* Laurence H. Tribe & Patrick O. Gudridge, *The Anti-Emergency Constitution*, 113 YALE L.J. 1801 (2004) (generally arguing that the Constitution should not apply any differently during times of war or national emergency).

72 WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 224–25 (1998).

73 United States v. U.S. Dist. Court, 407 U.S. 297, 316–17 (1972) (holding that the warrantless installation of a covert video recording device violates the Fourth Amendment). Note that *Katz* explicitly reserved judgment on a national-security exception to the Fourth Amendment. *See* Katz v. United States, 389 U.S. 347, 358 n.23 (1967).

74 *See* Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004) (striking down a portion of the USA PATRIOT Act authorizing a unique form of administrative subpoena called a "national security letter"); Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (holding that the Constitution still requires due process for American citizens captured in foreign countries and labeled enemy

notably issued its first published opinion, and in that opinion it purposely stated that a terrorist "emergency" qualifies under the "special needs test" as it is "out of the realm of ordinary crime control."[75] While it is true that a court's first opinion may not hold much persuasive authority, the court is populated by federal judges all of whom were appointed by the Chief Justice[76] and is therefore possibly quite persuasive indeed.[77]

Suffice it to say that while the Supreme Court has never specifically cited national security concerns as a special need that would circumvent normal Fourth Amendment procedures, there are at least indications that such an approach is possible. Assuming this is the case, what are the benefits of the doctrine? Obviously, the clarity that it provides to law enforcement is

---

combatants). While *Ashcroft* certainly addressed Fourth Amendment issues, it did so in the context of administrative subpoenas, which are ordinarily permissible so long as judicially observed and the subpoena is for a "search" falling outside of the Fourth Amendment's protections. *See Ashcroft*, 334 F. Supp. 2d at 495.

75 *In re* Sealed Case No. 02-001, 310 F.3d 717, 745–46 (FISA Ct. Rev. 2002) (per curiam), *abrogating sub nom. In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (FISA Ct. 2002).

76 *See* 50 U.S.C. § 1803 (2000). It is worth noting that the courts created by the Foreign Intelligence Surveillance Act, Pub. L. No. 95–511, 92 Stat. 1783 (1978) (codified as amended at 50 U.S.C.A. §§ 1801–1829 (West 2004)) [hereinafter FISA], are properly constituted Article III courts, despite their judges' lack of lifetime tenure on the tribunals. *See* John J. Dvorske, *Validity, Construction, and Application of Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.A. §§ 1801 et seq.) Authorizing Electronic Surveillance of Foreign Powers and Their Agents*, 190 A.L.R. FED. 385, § 5(a) (2005) (collecting cases).

77 On the other hand, annual reports filed by the U.S. attorney general under 50 U.S.C. § 1807 (2000) demonstrate the overwhelming deference shown to the government by the FISA courts: between 1996 and 2004, only *four* of 9,915 applications were denied. *See* Letter from Janet Reno, U.S. attorney general, to L. Ralph Mecham, director, Administrative Office of the United States Courts (Apr. 18, 1997), http://www.usdoj.gov/oipr/readingroom/fisa_ltr.htm; Letter from Janet Reno, U.S. attorney general, to L. Ralph Mecham, director, Administrative Office of the United States Courts (Apr. 29, 1998), http://www.usdoj.gov/oipr/readingroom/97fisa_ltr.htm; Letter from Janet Reno, U.S. attorney general, to L. Ralph Mecham, director, Administrative Office of the United States Courts (Apr. 29, 1999), http://www.usdoj.gov/oipr/readingroom/1998annualfisa reporttocongress.html; Letter from Janet Reno, U.S. attorney general, to L. Ralph Mecham, director, Administrative Office of the United States Courts (Apr. 27, 2000), http://www.usdoj.gov/oipr/readingroom/99fisa–ltr.html; Letter from John Ashcroft, U.S. attorney general, to L. Ralph Mecham, director, Administrative Office of the United States Courts (Apr. 27, 2001), http://www.usdoj.gov/oipr/readingroom/2000fisa–ltr.pdf; Letter from Larry Thompson, acting U.S. attorney general, to L. Ralph Mecham, director, Administrative Office of the United States Courts (Apr. 29, 2002), http://www.usdoj.gov/oipr/readingroom/2001fisa–ltr.pdf; Letter from John Ashcroft, U.S. attorney general, to L. Ralph Mecham, director, Administrative Office of the United States Courts (Apr. 29, 2003), http://www.usdoj.gov/oipr/readingroom/2002fisa–ltr.pdf; Letter from William E. Moschella, assistant U.S. attorney general, to L. Ralph Mecham, director, Administrative Office of the United States Courts (Apr. 30, 2004), http://www.usdoj.gov/oipr/readingroom/2003fisa–ltr.pdf; Letter from William E. Moschella, assistant U.S. attorney general, to L. Ralph Mecham, director, Administrative Office of the United States Courts (Apr. 1, 2005), http://www.usdoj.gov/oipr/readingroom/2004fisa-ltr.pdf.

head and shoulders above either the *Katz* or *Kyllo* tests. No interpretations of societal expectations of privacy or commonality of technology are necessary: risk to national security is the sole factor in determining whether a new technology could be constitutionally used in an anti–terrorism case. Unfortunately, the opposite side of the coin is just as clear: privacy protections, inadequate as some might interpret them under *Katz* or even *Kyllo*, are virtually nonexistent under this version of the legitimate governmental interests test. This is especially true when one considers that attacks on constitutional protections are at their height during times of national emergency,[78] creating a high potential for abuse.

II. The Test Case of Electronic Mail

Having laid out the three distinct constitutional standards that could be used to scrutinize the reasonableness of emerging surveillance technology under the Fourth Amendment, a concrete example is instructive. While the different tests might seem relatively understandable in general, it is only by understanding their usage in specific cases that the need for a new and uniform standard truly becomes clear. For reasons stated below,[79] the best technology to analyze the application of these three standards is the interception of e-mail.

A. Brief History of the Regulation of Communications Interception

One of the Supreme Court's first forays into the world of communications interception came in 1928 when it held that wiretapping did not qualify as a "search or seizure" under the Fourth Amendment because there was no physical intrusion.[80] Congress responded with a total prohibition on wiretapping with the Federal Communications Act of 1934.[81] After the Court scrapped the trespass doctrine finding that "the Fourth Amendment protects people, not places,"[82] some type of regulatory framework was neces-

78 *See supra* note 69 and accompanying text.

79 *See infra* text accompanying notes 104–19.

80 *See* Olmstead v. United States, 277 U.S. 438, 466 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

81 *See* Federal Communications Act, ch. 652, § 605, 48 Stat. 1103 (1934). However, in practical terms the ban on communications interception was anything but total. Its application was interpreted to have limited scope. *See* Richard C. Turkington, *Protection for Invasions of Conversational and Communication Privacy by Electronic Surveillance in Family, Marriage, and Domestic Disputes under Federal and State Wiretap and Store* [sic] *Communications Acts and the Common Law Privacy Intrusion Tort*, 82 Neb. L. Rev. 693, 701 (2004).

82 Katz v. United States, 389 U.S. 347, 351 (1967).

sary to enable law enforcement to use wiretapping technology in a manner consistent with notions of privacy and due process. Barely a year after the Court's ruling in *Katz*, Congress passed the Omnibus Crime Control and Safe Streets Act (OCCSSA),[83] Title III detailed the procedures for procuring a warrant to lawfully intercept communications.[84] It quickly became evident that the need for secrecy in investigations of foreign intelligence agents required a different warrant procedure; thus, Congress enacted FISA which provided an alternative to Title III warrants.[85] FISA has turned into one of the government's primary weapons in investigating terrorism.[86]

Roughly contemporaneous with the passage of FISA, the Supreme Court handed down several decisions dealing with pen registers, first finding that they fell outside the scope of Title III,[87] and shortly thereafter ruling that they fell outside the scope of the Fourth Amendment itself.[88] The early 1980s then ushered in the beginning of a new age of digital communications: the Internet and e-mail. What is presently known as the Internet began as a 1960s-era research project by the Advanced Research Projects Agency called ARPANet. The purpose of ARPANet was to provide a communications network that was resistant to nuclear attack.[89] In this manner, ARPANet is the historical antecedent of what are today called "packet-switched" communications networks as well as the direct predecessor of the Internet. In such networks, an e-mail or other digital communication is broken up into smaller "packets," each of which follows the "least cost path" principle in finding the shortest and fastest route to its target bypassing slow or malfunctioning message relay centers to be reconstituted at the message destination.[90] Responding both to the Court's pen register decisions and the unprecedented explosion of new communications technology, Congress passed the Electronic Communications Privacy Act (ECPA) in 1986.[91] ECPA substantially amended Title III of OCCSSA separating it into three new provisions: Title I, which covers content interception ofelec-

83 Omnibus Crime Control and Safe Streets Act, Pub. L. No. 09–351, 82 Stat. 197–239 (1968) [hereinafter OCCSSA]. OCCSSA is also notable in that it was the first federal law to provide block grants for law enforcement. *See* OCCSSA §§ 510–18 (codified as amended at 42 U.S.C. §§ 3760–64 (2000)).

84 *See* OCCSSA § 802 (codified as amended at 18 U.S.C. §§ 2510–20 (2000)).

85 *See* FISA, Pub. L. No. 95–511, 92 Stat 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801–29, 1802 (2000)).

86 *See, e.g., In re* Sealed Case No. 02–001, 310 F.3d 717, 746 (FISA Ct. Rev. 2002).

87 *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 165–66 (1977).

88 *See* Smith v. Maryland, 442 U.S. 735, 742 (1979).

89 *See* Reno v. ACLU, 521 U.S. 844, 850 (1997).

90 *See generally* Holland, *supra* note 11, at 17–18. It should be noted that this is a woefully short and technically inaccurate description of the Internet, but it suffices for the purpose of understanding the troubled status that electronic communications hold in the courts.

91 Electronic Communications Privacy Act, Pub. L. No. 99–508, 100 Stat. 1848 (1986) [hereinafter ECPA].

tronic communications,[92] Title II, which regulates the acquisition of stored communications,[93] and Title III, which governs the use of noncontent pen registers and trap and trace devices.[94]

Congress would respond twice more to the growing demand for electronic surveillance in an increasingly technology-assisted world. In 1994, it passed the Communications Assistance to Law Enforcement Act (CALEA) which partially amended ECPA and required telecommunications carriers to cooperate with law enforcement by making their system architecture amenable to easy tapping.[95] CALEA was soon held to apply to Internet service providers (ISPs) requiring them to install technology on their servers that would allow for the interception of digital packet-switched data.[96] Then came the tragic events of September 11, 2001 and the now-famous congressional response, the nationalistically named USA PATRIOT Act.[97] The USA PATRIOT Act amended ECPA to include specific statutory authorization to intercept packet-switched communications.[98] Despite the objections of some commentators, such authorization had simply been inferred prior to the USA PATRIOT amendment.[99]

Thus, the regulatory landscape of e-mail is at this point thoroughly muddled. A law enforcement officer seeking to snoop through a suspected terrorist's e-mail has the option of acquiring a Title I content warrant,[100] a Title II stored communications order,[101] a Title III pen register order,[102] or a FISA warrant,[103] all without running afoul of the Fourth Amendment's prohibition on warrantless searches. Unfortunately, as will be shown below, the legal status of e-mail under the Fourth Amendment is not nearly so cut and dried. If e-mail, a technology that has existed for decades and

92 *See* ECPA §§ 101–11 (codified as amended at 18 U.S.C. §§ 2510–21 (2000)).

93 *See* ECPA § 201 (codified as amended at 18 U.S.C.A. §§ 2701–11 (West 2004)). Some courts speak instead of the Wiretap Act or the Stored Communications Act, which are actually references to ECPA Titles I and II, respectively. *See* TURKINGTON & ALLEN, *supra* note 4, at 231.

94 *See* ECPA § 301 (codified as amended at 18 U.S.C. §§ 3121–27 (2000)).

95 *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103–414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 U.S.C. and 47 U.S.C.) [hereinafter CALEA].

96 *See* United States Telecom Ass'n v. FCC, 227 F.3d 450, 464–65 (D.C. Cir. 2000).

97 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107–56, 115 Stat. 272 (2001) [hereinafter USA PATRIOT].

98 *See, e.g.*, USA PATRIOT § 216 (codified at 18 U.S.C. § 3121 (2000)).

99 *See* Thomas R. McCarthy, *Don't Fear Carnivore: It Won't Devour Individual Privacy*, 66 MO. L. REV. 827, 842 (2001).

100 *See* 18 U.S.C. § 2518(3) (2005).

101 *See* §§ 2703(a)–(d).

102 *See* § 3123(a).

103 *See* 50 U.S.C. § 1804(a) (2000).

has been in increasingly common use in recent years, enjoys an uneasy relationship with the Fourth Amendment, then there seems to be little hope that emerging forms of technological surveillance will be uniformly analyzed by the courts.

B. Why E-Mail is a Representative Test Case

As was previously stated, the Internet has exploded in popularity in American households[104] and has become especially widespread in terrorist and criminal endeavors and investigations.[105] Despite this rampant popularity, the constitutional standards as applied to online communications are far from clear. Courts, perhaps due to an inherent inability to think in purely technological terms, have proven spectacularly ill suited to deal with packet-switched communications interceptions. Some examples are in order.

The first cases to be examined deal not with constitutional questions but address e-mail in the employment context. In an unreported tortious-invasion-of-privacy case, a Microsoft employee was held not to have a reasonable expectation of privacy in personal e-mails stored in password-protected folders on an office computer.[106] The plaintiff in another case had been assured of the utter confidentiality of his e-mail communications by his employer (the plaintiff was using a corporate e-mail address) yet was still fired due to the content of those e-mails. In his suit for wrongful discharge, the court held that an employee has no "reasonable expectation of privacy" in the content of his e-mails from an employee to his supervisor.[107] Again, while these are not constitutional cases, it is curious that the courts used language similar to or lifted straight from *Katz* to describe the plaintiffs' e-mail privacy (or lack thereof, as the cases held). This represents a fundamental misunderstanding of the nature of e-mail. If the plaintiffs in the two cases had made the comments at issue on written letters sealed and sent via a company interoffice memo network, it would be difficult to imagine a court coming to the conclusion that they had no reasonable expecta-

104 *See* Nat'l Telecomms. & Info. Admin., A Nation Divided: Entering the Broadband Age fig. 1 (2004), http://www.ntia.doc.gov/reports/anol/NationOnlineBroadband04.htm (by October of 2003, 54.6% of U.S. households had Internet access, nearly three times the number in October of 1997).

105 *See Hearings*, *supra* note 13. The prevalence of Internet-based investigations is somewhat conjectural. *Compare* United States v. Harvey, No. 51-4:02 CR 482JCHDDN, 2003 WL 22052993, at * 3 (E.D. Mo. July 28, 2003) (stating that the case involved only the second request ever for a warrant under Title I of ECPA), *with* FEDERAL BUREAU OF INVESTIGATION, CARNIVORE/DCS-1000 REPORT TO CONGRESS 2 (2003), http://www.epic.org/privacy/carnivore/2003_report.pdf (indicating that FBI e-mail surveillance technology was authorized under Title I twice in 2003, and under Title III six times).

106 *See* McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *4 (Tex. App. May 28, 1999).

107 *See* Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996).

tion of privacy in the contents of those sealed messages. The fact that the messages could be viewed by those with the requisite technical expertise should not change the fact that the plaintiff still had an expectation that they would not be so viewed. As one court aptly noted, "[t]he mere possibility that interception of the communication is technologically feasible does not render public a communication that is otherwise private."[108] To date, only one court has explicitly ruled that there exists a Fourth Amendment reasonable expectation of privacy in the content of e-mailed messages.[109] However, probably because the decision was handed down by a military appeals court, its use in the civilian courts has been rare.[110]

Several other cases concern confusion with the methods of e-mail delivery, again indicating a basic misunderstanding of technological functionality. First, at least two courts have ruled that under state statutory analogues to ECPA, a sender of e-mail implicitly consents to its recording by law enforcement as e-mail is inherently a recorded medium (as opposed to verbal conversations over a telephone line).[111] The implication of such rulings is clear: the interception of *any* digital communication to another computer would be impliedly consented to, and therefore, the sender would have no

108 State v. Townsend, 57 P.3d 255, 259 (Wash. 2002); *see also* Max Guirguis, *Electronic Mail Surveillance and the Reasonable Expectation of Privacy*, 8 J. TECH. L. & POL'Y 135, 153–54 (2003) ("Simply stated, the Court may use the lack of security during the transmission of messages and the dramatic rise in hacking and computer crime as reasons to withhold Fourth Amendment protection altogether from e-mail messaging. Though consistent with the Court's holdings in the area of privacy, this rationale bases the reasonableness of the users' privacy expectations almost exclusively on the drawbacks in the existing technology or on the limitations of the informational infrastructure.").

109 *See* United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996), *aff'd* 46 M.J. 413 (C.A.A.F. 1997). Even this holding is itself limited, as the same court later held that ISP records of customers' visited websites were transactional records not protected from warrantless searching by the Fourth Amendment. United States v. Allen, 53 M.J. 402, 409 (C.A.A.F. 2000), *cert. denied*, 532 U.S. 907 (2001); *cf. Miller*, 425 U.S. at 443 (bank transactional records fall outside the Fourth Amendment). *Allen* is yet another example of judicial misunderstanding of technology, because even though web surfing is not literally identical to e-mail, from a technological standpoint the two are essentially indistinguishable—both methods of communication involve nothing more than the exchange of packetized digital data.

110 Although *Maxwell* has been extensively cited in law journal articles and treatises, only eight civilian courts have ever cited it, and none of them have gone so far as to *follow* it, holding for various reasons that there was no reasonable expectation of privacy in the electronic communication in question. *See, e.g.*, *Townsend*, 57 P.3d at 263; Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. Ct. 2001), *aff'd per curiam without opinion*, 837 A.2d 1163 (Pa. 2003) (per curiam).

111 *See Townsend*, 57 P.3d at 260 ("In sum, because Townsend, as a user of e-mail had to understand ... that his e-mail messages would be recorded on the computer of the person to whom the message was sent, he is properly deemed to have consented to the recording of those messages."); *Proetto*, 771 A.2d at 829 ("Any reasonably intelligent person, savvy enough to be using the Internet, however, would be aware of the fact that messages are received in a recorded format, by their very nature, and can be downloaded or printed by the party receiving the message.").

reasonable expectation of privacy in the communication's contents. Such a finding would be contrary to any contemporary notions of privacy[112] as well as congressional understanding.[113] In another case, federal agents seized a computer that was being used as a message server storing messages for later retrieval by an e-mail system's users. The contents of that computer were seized under the less stringent provisions of Title II as they were seen as stored communications.[114] At first blush, this seems to be patently obvious. However, viewing all third party message servers as storage devices for Title II purposes overlooks the entire nature of packet-switched networks such as the Internet. E-mails are not like telephone calls which are terminated if the recipient does not respond. Unless an e-mail recipient's computer is on and actively receiving packets at the time the e-mail arrives, it must necessarily be placed in electronic storage on some third party's system.[115] The process can roughly be analogized to delivery of ordinary mail via the U.S. Postal Service in which letters are considered in transit until actually delivered.[116] Essentially, the court in the above case would label a vast portion of the world's daily e-mail traffic as in storage rather than in transit and therefore susceptible to interception under Title II of ECPA.[117] A similar and more recent ruling is potentially even more disastrous for proponents of digital privacy. In *United States v. Councilman*, the First Circuit recently held that an ISP administrator who intercepted and copied all e-mails to his customers originating from one of his competitors did not violate Title I's prohibition on unauthorized interceptions because the e-mails were, if only for a period measured in fractions of a second, in the ISP's possession.[118] As it stood, the *Councilman* decision signaled the end of online communications privacy. It would allow law enforcement agents to

112 *See* Larry O. Natt Gantt II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 347 (1995).

113 Given that Congress amended ECPA specifically to prohibit interception of packet-switched communications without proper judicial authorization, *see* USA PATRIOT, *supra* note 98, it is indeed bizarre that the courts would find that the Internet users had consented to the interception of those communications.

114 *See* Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 458–59 (5th Cir. 1994).

115 *See* Bohach v. City of Reno, 932 F. Supp. 1232, 1234 n.2 (D. Nev. 1996).

116 *See generally* Timothy Coughlan, *Applying the U.S. Postal Service Statutes to E-Mail Transmissions*, 25 RUTGERS COMPUTER & TECH. L.J. 375 (1999).

117 See United States v. Smith, 155 F.3d 1051, 1058 (9th Cir. 1998) for an example of a court that came to the conclusion that Titles I and II should be interpreted together and not applied to different situations based on technical minutiae.

118 *See* United States v. Councilman, 373 F.3d 197, 203–04 (1st Cir. 2004), *reh'g en banc granted*, 385 F.3d 793 (1st Cir. 2004), *and vacated*, 418 F.3d 67 (1st Cir. 2005). Since there was no contemporaneous interception, the defendant's actions fell outside the prohibitions of Title I and were instead covered by Title II. *See id.* at 203 (citing *Steve Jackson Games*, 36 F.3d. at 462). Title II does not prohibit ISPs from accessing stored communications. 18 U.S.C. §§ 2701(a), (c)(1).

access the contents of e-mail without a warrant in seemingly flagrant violation of the Fourth Amendment because the courts have proven incapable of adapting themselves to changing technological climes. The fact that the court reheard the case en banc and reversed itself[119] is largely immaterial to the underlying difficulty: courts have time and again proven themselves incapable of resolving legal issues centered around new technological developments. It is in this context that e-mail monitoring, along with other surveillance technologies, should be examined anew under the Fourth Amendment. If a relatively stable and longstanding technology is subject to such treatment, then there would appear to be little if any guidance on how revolutionary new technologies will be treated by the courts.

C. The Carnivore Internet Monitoring Device

Due to the obvious need for a technology that assists law enforcement in monitoring electronic communications, the FBI developed a device known as Carnivore.[120] Carnivore is capable of functioning in multiple modes, only two of which need be addressed here: content interception mode, in which the content of e-mail, online chatroom conversations, and website visits is recorded, and noncontent addressing interception mode, in which the "to:" and "from:" lines of e-mails and the website addresses visited are recorded.[121] Since Carnivore is precisely the type of device that should be in mind when considering how the Fourth Amendment applies to technological breakthroughs, its capabilities will be examined under each of the standards listed above.

If courts manage to avoid the *Councilman* pitfall of applying obsolete statutory metaphors to new technology,[122] modeling Carnivore as a trad-

119 *See* United States v. Councilman, 467 F.3d 67 (1st Cir. 2005) (en banc).

120 *See* Neil King, Jr. & Ted Bridis, *FBI's Wiretaps to Scan E-Mail Spark Concern*, WALL ST. J., July 11, 2000, at A3. The specific hardware and software known as Carnivore (or DCS1000, the name adopted for Carnivore after it became public; *see* McCarthy, *supra* note 99, at 828 n.5) is no longer in use by the FBI, but commercial tools that better perform the same functions as Carnivore have replaced it. *See* Ted Bridis, *FBI Abandons Its Software for Online Wiretaps; Bureau Switching to Commercial Snooping System*, CHI. TRIB., Jan. 19, 2005, at 12.

121 *See* ILL. INS. OF TECH. RESEARCH INST., INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM: FINAL REPORT 3–24 to 3–28 (2000), http://www.usdoj.gov/jmd/publications/carniv_final.pdf; *see also* Holland, *supra* note 11, at 6–12.

122 *See* Stephanie A. Gore, *"A Rose by Any Other Name": Judicial Use of Metaphors for New Technologies*, 2003 U. ILL. J.L. TECH. & POL'Y 403, 455 (2003):

> Metaphors should be the jumping-off point for understanding new technologies, not a substitute for such understanding. The challenge for courts is to become more attentive in using metaphors to understand new phenomena. As a number of commentators have advised, courts and policymakers must take into account the differences between the Internet and the physical world when formulating legal policies for this new medium.

tional wiretapping device seems to fit squarely into the *Katz* and *Kyllo* regimes. Under *Kyllo*, e-mail can certainly be said to be in general public use. However, it is not the e-mail itself but Carnivore, an e-mail interception device known as a packet sniffer,[123] that is the relevant technological device. This is precisely the difficulty that lies in applying *Kyllo*: determining at what point a device, which is undeniably publicly available,[124] becomes a device in general public use. A similar problem applies when analyzing Carnivore as a content interception device under *Katz*. That society exhibits a subjective expectation of privacy in the content of its e-mails is incontrovertible, but whether it views that expectation as reasonable based on the fact that competent technicians can in fact access its e-mails at any time can certainly be called into doubt.[125] An even larger unknown is whether the Supreme Court would find society's privacy expectation to be reasonable. The question then becomes whether a person can have a reasonable expectation of privacy when using a technology known to be capable of interception.[126] Since all forms of communication are susceptible to some type of unwanted third party interception, it would seem that *Katz* would require a warrant to intercept the contents of e-mail communications, but the fact remains that the constitutional issue has never been directly addressed by the Supreme Court. This lack of clarity on such a basic issue is precisely why a new standard is necessary.

Analyzing Carnivore as a pen register device is even more complicated under either *Katz* or *Kyllo*. It should be noted that there is considerable dissent over the basic issue of the Fourth Amendment's inapplicability to pen registers, as several state appellate courts have ruled that their state constitutions provide broader protections than the Fourth Amendment and have embraced a reasonable expectation of privacy in the information gleaned

---

See also Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 875–76 (2004) ("Judges struggle to understand even the basic facts of [new] technologies, and often must rely on the crutch of questionable metaphors to aid their comprehension.").

123 *See supra* note 11 and accompanying text.

124 Packet sniffers are routine tools for network maintenance, entirely unrelated to their possible uses as snooping devices. *See* WIKIPEDIA, PACKET SNIFFERS, http://en.wikipedia.org/wiki/Packet_sniffer (last visited Sept. 27, 2005).

125 *But see* Helen W. Gunnarsson, *Should Lawyers Use E-Mail to Communicate with Clients?*, 92 ILL. B.J. 572, 572–75 (2004) (citing with approval ABA Comm. on Ethics and Prof'l Responsibility, *Protecting the Confidentiality of Unencrypted E-Mail*, Formal Op. 99-413 (1999) ("A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a *reasonable expectation of privacy* from a technological and legal standpoint.") (emphasis added)).

126 The Court has exhibited some receptiveness to the argument that the mere *possibility* of loss of privacy eliminates the reasonableness of an expectation thereof. *See* California v. Greenwood, 486 U.S. 35, 40–41 (1988).

by pen register devices.[127] Carnivore merely exacerbates this controversy because the "pen register" information it records is often much more content-like than the dialed numbers intercepted under a traditional pen register and reveals significantly more information about the person.[128] The same difficulties with applying the *Kyllo* test to content interceptions of e-mail apply to Carnivore's pen register mode, but the *Katz* analysis is somewhat different due to the Supreme Court's prior rulings on pen registers.[129] Since the Court accepts as a given that information voluntarily turned over to a third party even for specifically limited purposes is constitutionally unprotected, the *Katz* analysis is over. However, if the Court could be convinced that "routing" and "addressing"[130] information of the type collected by Carnivore in pen mode were of a type creating a reasonable expectation of privacy, then the same intractable difficulties that applied in the content interception stage once again apply. In short, under both *Katz* and *Kyllo*, it is at best difficult to predict just how the Fourth Amendment will be applied to new technologies.

It would seem then that the only existing solution that would provide adequate guidance on either of Carnivore's operational modes or on any other new surveillance technologies would be the national security special needs test. Unfortunately, accepting national security as a legitimate governmental interest eviscerates privacy.[131] While the lack of clarity and guidance to law enforcement on future technologies inherent in the *Katz* and *Kyllo* tests is eliminated in the legitimate governmental interests test, the lack of privacy protections and potential for abuse become even greater when concerning a technology as widespread as e-mail. Thus, it appears that none of the three Fourth Amendment standards adequately balances

127 *See* People v. Blair, 602 P.2d 738, 746–47 (Cal. 1979); People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983); State v. Hunt, 450 A.2d 952, 956–57 (N.J. 1982); Richardson v. State, 865 S.W.2d 944, 954 (Tex. Crim. App. 1993); State v. Gunwall, 720 P.2d 808, 813 (Wash. 1986). Not all states take such an approach. *See, e.g.*, Holbrook v. Knopf, 847 S.W.2d 52, 55 (Ky. 1992) (holding that Section 10 of the Kentucky Constitution is "interpreted coextensively" with the Fourth Amendment).

128 *See* Holland, *supra* note 11, at 37–39. This point is best shown by comparing telephone pen register information to electronic routing pen register information in the following example. Assume that John Doe is the target of an FBI investigation, with both a traditional telephone pen register and a Carnivore-like pen register recording his actions. Were Doe to call a bookstore to order a book, the only information gained by the FBI would be that Doe dialed the bookstore's number at a certain time. However, if Doe instead visited an online bookseller to order the same book, Carnivore would record every separate page visited, thus allowing the FBI to discover every piece of information that Doe looked at (including the type of book that Doe is generally interested in), in addition to what book he actually purchased. Title III's characterization of this as noncontent information is strikingly flawed. *Contra* 18 U.S.C. § 3121(c) (2000).

129 *See supra* notes 87–88 and accompanying text.

130 *See* § 3121(c).

131 *See supra* note 73 and accompanying text.

privacy and security. If both privacy and security are to be protected in light of the Fourth Amendment, a new constitutional doctrine is in order.

III. Proposal for a Merged Fourth Amendment Standard to Apply to Emerging Technology

This Note proposes a new merged standard combining the best aspects of the three aforementioned doctrines. The merged standard applies differing constitutional standards at three separate stages. In the first stage, when a technology is truly new (in other words, when it has seen no or extremely limited public availability)[132] the use of that technology to conduct surveillance would be analyzed under a *Kyllo*-like approach but one that applies not just to homes. Put in different terms, when a new surveillance technology is first emerging, it cannot be used without a warrant. Once the technology becomes relatively common, a modified version of the *Katz* reasonable expectation of privacy test is applied in the second stage. For all its faults, *Katz* is bound up in years of precedent, and scrapping a decades-old constitutional doctrine in the interests of greater predictability would be counterintuitive. However, here the *Katz* test would be applied with considerably more deference to privacy by focusing on *actual* societal manifestations of an expectation of privacy rather than on the objective criteria on which the expectation is currently gauged.[133] Finally, the third stage: the technological surveillance technique has passed into frequent usage by the public, causing the expectation of privacy from such a technique to be considered per se unreasonable and allowing such searches to be conducted entirely outside the Fourth Amendment.

The multiple stages of scrutiny set forth above are only the first of two major elements of the merged standard. While the first element incorporates aspects of the *Katz* and *Kyllo* tests and is aimed at maximizing privacy, the second element integrates the special needs test into the first element and is aimed at maximizing security. In each stage of the merged

132 "Public" as used in this context simply means non–law enforcement and intelligence officials.

133 Again, Justice Harlan's reasonableness test had two factors: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The plain import of this language is that an individual's subjective expectation of privacy must be supported by society's concurrence in order for that expectation to be reasonable. However, the Court has morphed this into a requirement that both individual *and* societal expectations of privacy be objectively reasonable. "An expectation of privacy does not give rise to Fourth Amendment protection, however, unless society is prepared to accept that expectation as *objectively* reasonable." California v. Greenwood, 486 U.S. 35, 39–40 (1988) (emphasis added); *see also* California v. Ciraolo, 476 U.S. 207, 209–10 (1986) (describing "objective criteria" used to judge an individual's subjective manifestation of privacy).

standard, a separate analysis applies when national security is the asserted justification for the use of the search technology. At the first stage, when the constitutional privacy protections are at their peak, there is obviously a concurrent necessity for adequate security protections. Therefore, if search technologies new enough to require a warrant in ordinary investigations are used in a national security context, a rebuttable presumption arises that the search is reasonable. Essentially, in the first stage any national security search conducted without a warrant is saved from an arbitrary finding of unconstitutionality by this presumption, albeit one that can be overcome to prevent its abuse when the justification is merely pretextual. In the second stage, the *Katz*-like analysis does not give rise to nearly as high a requirement for a security exemption as existed in the first stage. Consequently, instead of an automatic rebuttable presumption of constitutionality, a security-justified search using second stage technology would only require such a presumption when the societal expectation of privacy is neither clearly present nor clearly non-existent. The rebuttability of the presumption would still provide protection for privacy when the national security justification was pretextual, and the added requirement that the expectation of privacy be doubtful ab initio further protects individuals from rationalized encroachments on their privacy.[134] Finally, in the third stage of the merged standard the complete exception of the search technology from the Fourth Amendment simultaneously eliminates the need for any special security analysis.

There are several benefits to using the merged standard above. First and foremost, the standard would be known and more predictable, whereas currently the Supreme Court could apply any one of three possible standards without much if any warning. Additionally, the standard balances both privacy and security in a way that allows them primacy over the other only when such prevalence would be based on objectively identifiable factors and not according to shifting societal views of privacy.[135] A constitu-

134 Of course, protection of individual privacy and assurance of national security are not the only considerations of the security aspect of the merged standard. Protection of sources and methods of intelligence gathering is also of critical import. It is for reasons such as this that the President's authority to conduct warrantless searches in the gathering of foreign intelligence had been recognized prior to the enactment of FISA. *See* United States v. Truong, 629 F.2d 908, 913–14 (4th Cir. 1980) (warrantless searches that took place prior to FISA's 1978 enactment not unconstitutional). FISA was passed in part because of the need for a "secure framework by which the Executive Branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights." S. REP. No. 95–604, at 15 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3916; *see also* 50 U.S.C. § 1803(c) (2000). Therefore, it would seem that requiring any security analysis under the merged standard to be raised exclusively in the Foreign Intelligence Surveillance Court would be the only way to adequately safeguard national secrets.

135 Arguably, any *Kyllo*-like analysis suffers from a similar defect, making an expectation of privacy dependent upon "market forces," in effect substituting "substantial sales" for

tional expectation of privacy dependent upon the present state of technology would create a much more rational correlation between subjective expectations and those recognized by the Court. Since courts have proven themselves ill suited to rule on technologies so new that the general public does not understand them, the merged standard eliminates the necessity of judicial understanding of the underlying technology.[136] A court need not know how e-mail travels on a packet-switched network in order to understand that packet sniffers are not in frequent everyday use but are readily publicly available and that their use must therefore be subject to a second stage *Katz*-like finding of reasonableness. Finally, concentrating a reasonableness finding on societal recognitions of privacy would return Fourth Amendment analysis to what Justice Harlan actually stated in *Katz* as opposed to the objective standard of more recent cases.[137]

Of course, there are certainly problems to be resolved with the merged standard. First, it suffers from the same defect as the *Kyllo* test yet amplified: determining at what exact point a technology passes into "common" and "frequent" use. However, under the merged standard these are evidentiary difficulties as opposed to the definitional ambiguity in the *Kyllo* "general public use" standard.[138] Also, the merged standard is undeniably more intrinsically complicated than any of the three current doctrines are separately. More complicated does not necessarily mean more precise. Since, as a general rule, clearer rules provide for more predictable decisions,[139] courts should strive for clarity in their decisions. However, despite the merged standard's complexity, its utilization of observable distinctions between different classes of cases makes for an overall doctrine that is clearer than the combination of possible Fourth Amendment analyses currently used. Still, the main point on which the merged standard could be assailed is its national security search exemption aspect, as such solici-

societal expectations. William C. Heffernan, *Fourth Amendment Privacy Interests*, 92 J. CRIM. L. & CRIMINOLOGY 1, 102–03 (2002). This is certainly a valid critique of *Kyllo* within the *Katz* framework, but its efficacy would actually be an argument in *favor* of the merged standard's approach. "Substantial sales" cannot occur without generalized public consent, generating precisely the type of verifiable indicia of public usage that the merged standard looks for in categorizing a technology.

136 To be sure, the fact that a judge is personally competent in the use of some type of technology would seem to indicate a higher level of societal use than is required in the first stage. However, personal judicial familiarity would be unnecessary, as statistical data and expert testimony could fairly accurately demonstrate the level of public use. Similarly, judicial awareness of a particular technology may lead to the use of judicial notice to determine in which stage of the merged standard the technology lies. *See generally* FED. R. EVID. 201.

137 *See supra* note 133.

138 *See supra* notes 135–36.

139 *See* Antonin Scalia, *The Rule of Law as a Law of Rules*, 56 U. CHI. L. REV. 1175, 1179 (1989) (noting that clear rules enhance predictability, an essential aspect of the rule of law).

tousness towards governmental powers is unsettling.[140] Unfortunately, an adequate balance between privacy and safety necessarily requires some consideration of security accommodations. The benefit of the security facet of the merged standard is that it is both surmountable and inherently conditional in contrast to the categorical national security exception that the current legitimate governmental interests test could give rise to. The potential for abuse under the latter standard is clear while the former presents significant hurdles to possible exploitation of a security loophole in the Fourth Amendment. Finally, the total lack of constitutional privacy protections in the third stage could be seen as a major deficiency, but the purpose of the third stage abrogation is to allow societal expectations of privacy to express themselves via Congress in the form of privacy-protecting legislation. In this manner, privacy advocates need not fear nullification of Fourth Amendment rights with every shift in the Court's membership. If American society truly values a certain aspect of privacy, they can depend on their elected representatives to protect it rather than an often unpredictable judiciary.[141]

IV. Conclusion: The Necessity For a Middle Ground

This Note emphasizes the necessity of clear guidance on Fourth Amendment treatment of new technology. Predictability is key for two reasons. Americans' privacy interest is one key reason: if we are to be snooped upon, we would prefer to know the circumstances under which snooping may occur. However, clarity and predictability in this area are most critical to law enforcement agencies, a fact that is best explained by relating past events. In early 2000, FBI agents investigating an American terrorist cell associated with Osama bin Laden were using Carnivore to track the cell's online communications.[142] One day, Carnivore somehow malfunctioned and intercepted the e-mails of people who were not targets of the investigation. Perhaps

140 *See supra* notes 67–78 and accompanying text.

141 "Some delay in the law is understandable given that the law is reactive and legislatures... cannot anticipate all the problems associated with new... technologies." Gantt, *supra* note 112, at 347–48. Despite what can sometimes be a ponderously slow legislative response, the fact remains that Congress has seen fit to respond to technological developments numerous times. *See supra* notes 38, 83, 91, 95, and 97 and accompanying text; *see also* Controlling the Assault of Non-Solicited Pornography and Marketing Act, Pub. L. No. 108–187, 117 Stat. 2699 (2003) (codified at scattered sections of Titles 15, 18, & 28 U.S.C.).

142 *See* Memorandum from [name redacted], Dep't of Justice Office of Intelligence Policy and Review, to Marion Bowman, FBI Assoc. Gen. Counsel for Nat'l Sec. Affairs (Apr. 5, 2000), http://www.epic.org/privacy/carnivore/fisa.html [hereinafter Memo]; *see also* Press Release, Elec. Privacy Info. Ctr., FBI's Carnivore System Disrupted Anti-Terror Investigation (May 28, 2002), http://www.epic.org/privacy/carnivore/5_02_release.html (explaining acronyms in and background information pertaining to the memorandum).

believing this to have violated the statutory minimization requirement[143] and thus rendering all the properly intercepted data inadmissible,[144] the law enforcement official running the Carnivore device at that time erased all the intercepted e-mails.[145] We will never know what intelligence was contained in those e-mails including whether it could have provided warning of future terrorist attacks. We will also never know whether a court would have allowed the already-intercepted e-mails to be entered into evidence.[146] What matters is that the courts' lack of predictability on Fourth Amendment matters was a direct cause of the loss of potentially vital national security information. If national security is to be protected, both private citizens and law enforcement must be at least generally aware of how the courts treat technology under the Fourth Amendment. The merged standard is designed, at least in part, to eliminate any possible confusion and make it impossible for another mishap like that noted above to occur.

A few specific examples should illustrate the workings of the merged standard. Search technologies such as the *Kyllo* thermal imagers or Voice over Internet Protocol (VoIP) surveillance devices[147] can be considered prototypical first stage technologies, while packet sniffers like Carnivore are properly categorized as second stage devices due to their relative commonality in the private sector.[148] Thus, while electronic surveillance of VoIP conversations would necessarily require a warrant, snooping on e-mail, instant messaging, and other forms of packetized communications would be analyzed under the merged standard's modified *Katz* test. In the interests of clarity, it should be made apparent that under this version of the *Katz*

143 *See* 50 U.S.C. §§ 1801(h), 1804(a)(5) (2000). Title I contains similar minimization requirements; *see* 18 U.S.C. § 2518(5) (2000).

144 *Cf.* Scott v. United States, 436 U.S. 128, 139–43 (1978) (holding that minimization requirements are aspects of Fourth Amendment reasonableness and are to be determined in a multifactor analysis). This decision has been highly criticized for failing to adequately protect privacy. *See* TURKINGTON & ALLEN, *supra* note 4, at 308–09 (citing Michael Goldsmith, *The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 97–112 (1983)).

145 *See* Memo, *supra* note 142.

146 It is worth noting that the exclusionary rule is inapplicable to evidence obtained in violation of Title III, as pen registers are not covered by the Fourth Amendment. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979). Curiously, while the constitutional exclusionary rule does apply to evidence taken in violation of Title I, there is also an explicit statutory exclusionary rule applicable to Title I. *See* 18 U.S.C. § 2515 (2000). Title III, by contrast, contains no comparable statutory exclusion.

147 VoIP is a relatively recent communications tool allowing for Internet telephony. The FCC is considering making VoIP providers subject to CALEA. *See* Proposed Rules, 69 Fed. Reg. 56,976, at 56,977–79 (Sept. 23, 2004) (to be codified at 47 C.F.R. pts. 22, 24, and 64). The FCC is already cooperating with Internet security specialists to develop a suitable form of VoIP wiretap. *See* Stephen Labaton, *F.C.C. Supports Surveillance Rules on Internet Calls*, N.Y. TIMES, Aug. 5, 2004, at C1.

148 *See supra* note 124 and accompanying text.

reasonableness test, both content and non-content "addressing" Internet communications would be subject to Fourth Amendment protections.[149] Breath-analysis sobriety tests and narcotics- and explosive-detecting canines (as well as their obvious electronic analogues)[150] present a contrary conclusion due to the well-known permissibility of their use by law enforcement.[151] While there is generally a subjective reasonable expectation of privacy for automobile trunks,[152] the fact that the public is largely aware of capabilities of sobriety tests and drug-sniffing dogs vitiates against that same expectation being applied to sniffing searches.[153] Lastly, the "frequent" use envisioned for third stage technologies would include only widely used tools such as digital cameras, answering machines, and binoculars, as well as low or no-tech surveillance techniques (for example, putting a glass to the wall in order to hear conversations occurring on the other side of it).[154] The critical distinction between third-stage devices and practices and those from which an expectation of privacy is lacking in the second

149 Applying the more privacy-oriented version of the *Katz* reasonableness test, *see supra* note 133 and accompanying text, individual and collective expectations of privacy in Internet communications are judged based on objectively verifiable manifestations, *see, e.g., supra* note 125, but are not subject to any further objective standards of reasonableness. *Cf. supra* note 108 and accompanying text.

150 *See* Richard J. Colton & John N. Russell, Jr., *Making the World a Safer Place*, SCIENCE, Feb. 28, 2003, at 1324 (noting chemical, biological, and radiological detectors in regular use at airports and major events).

151 *See* Schmerber v. California, 384 U.S. 757, 771–72 (1966) (mandatory breathalyzer testing based on a police officer's reasonable suspicion of drunken driving not prohibited by Fourth Amendment); *see also* United States v. Place, 462 U.S. 696, 707 (1983) (drug-sniffing canine use is *sui generis* in that it "discloses only the presence or absence of narcotics, a contraband item"); *accord* Illinois v. Caballes, 125 S. Ct. 834, 838 (2005) (citing *Place* in holding that sniff searches do not "implicate legitimate privacy interests").

152 *But see* Rakas v. Illinois, 439 U.S. 128, 148–49 (1978) ("[T]he trunk of an automobile ... [is an area] in which a passenger *qua* passenger simply would not normally have a legitimate expectation of privacy.").

153 However, the fact that the public is aware of the possibility that a communication will be intercepted is by no means determinative in finding a reasonable expectation of privacy. Cordless and cellular phones are illustrative on this point. It is generally understood that the technology to eavesdrop on cordless and cellular phone conversations is widely available. *See* Bartnicki v. Vopper, 532 U.S. 514, 522 n.6 (2001) ("[C]alls placed on cellular and cordless telephones can be intercepted more easily than those placed on traditional phones."); State v. McVeigh, 620 A.2d 133, 147 (Conn. 1993) ("[C]ordless telephone conversations ... are readily receivable by such commonplace items as ordinary television sets, baby monitors and other cordless telephones."). Still, a reasonable expectation of privacy in such communications clearly exists. *See Bartnicki*, 532 U.S. at 524 (noting that ECPA was expanded by CALEA to include both cordless and cellular phone conversations); United States v. bin Laden, 126 F. Supp. 2d 264, 281 (S.D.N.Y. 2000) (holding that there is a reasonable expectation of privacy in cellular phone conversations).

154 *Contra* People v. Arno, 153 Cal. Rptr. 624, 625 (1979) ("[T]he use of optical aids in the nature of binoculars, telescopes and the like is not itself determinative of the admissibility in evidence of the product of the observation ....").

stage is the regularity of use by private individuals as opposed to by law enforcement officials.[155]

Balancing privacy and security is no easy task. Legislatures, the courts, and commentators have attempted to find the proper balance for years, yet no universally accepted solution has yet been found. This merged standard of Fourth Amendment application to emerging technologies is far from comprehensive when it comes to the overall privacy-security balance. Still, any tool that would allow greater clarity in the law while preserving the flexibility that is so abundantly necessary in the law enforcement arena seems to be one which is moving in the right direction, in terms of the privacy-security balancing act. Effective Fourth Amendment jurisprudence must sometimes allow privacy to trump security and vice versa, but the situations in which one or the other may occur must not be declared according to nebulous political values.[156] Neither privacy nor security can always be favored because this would result in the other being abrogated to lesser status. The merged standard adopts a middle ground that will avoid this thereby strengthening attention to both privacy and security interests.

155 Note that while functionally speaking, there is little difference between these two areas, as neither is protected by the Fourth Amendment, there is an analytical justification for separating them. In the second stage's modified *Katz* analysis, if an individual does not possess a reasonable expectation of privacy from some surveillance mechanism, the chance will always exist that shifts in the state of the device's usage level will lead to its recategorization. In contrast, once a technology's commonality of use is sufficient to justify its inclusion in the third stage, any Fourth Amendment expectation of privacy is permanently revoked, making statutory protection the only alternative. *See supra* note 141 and accompanying text.

156 "Building on the special-needs cases would provide continuity of precedent and greater protection of individual privacy than would the construction of an entirely new and ad hoc catastrophic-threat or national-security exception to probable-cause requirements." Gould & Stern, *supra* note 71, at 831–32. Similarly, the merged standard approach would be less categorical than a special needs national security exception analysis, providing even more privacy protection.